AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

1. (Currently Amended) A method, comprising:

generating with a computer a set of subscriber-specific authentication data blocks into a network, each data block containing a challenge, a response and a key, where the generation is performed in the same manner as in a known mobile communications system;
transmitting with a transmitter at least some of the challenges contained in the authentication data blocks to a terminal;
choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification [[unit]] device of the terminal essentially in the same way as in a subscriber identification module of the mobile communication system;
determining an authenticator with an aid of the chosen key in the terminal;
transmitting, from the terminal to the network, the authenticator and [[a]] data [[unit]], the data [[unit]] containing information relating to the manner in which the authentication is formed and notifying the network with the aid of the data [[unit]] of which key corresponding to which challenge was chosen, and a check value with the aid of the chosen key in the network; and
comparing the check value with the authenticator.

2. (Currently Amended) The method as defined in claim 1, where the data [[unit]] is a security parameter index in the registration message of a mobile internet protocol.

3. (Currently Amended) The method as defined in claim 1, where the value of the response determined at the terminal is inserted into the data [[unit]]

4. (Currently Amended) The method as defined in claim 1, where the challenges are sorted in an order at the terminal with the aid of predetermined sorting criteria and a consecutive number corresponding to the chosen challenge is inserted into the data [[unit]].

5. (Currently Amended) The method as defined in claim 1, where the identification [[unit]] device used in the terminal is a subscriber identity module used by a global system for mobile communication system and the authentication data blocks are authentication triplets used by the global system for mobile communication system.

6. (Previously Amended) The method as defined in claim 5, where the authentication triplets are fetched from an authentication center of the global system for mobile communication system.

7. (Previously Amended) The method as defined in claim 6, where the challenges to be transmitted to the terminal are transmitted by using a short message switching service.

8. (Previously Amended) The method as defined in claim 1, where the challenges to be transmitted to the terminal are transmitted in an internet protocol datagram to be sent through an internet protocol network.

9. (Currently Amended) The method as defined in claim 1 for an internet protocol network, where the authentication data blocks are transmitted to a home agent of the terminal and with the aid of a data [[unit]] message the home agent is informed about which key corresponding to which challenge was chosen, where the check value is determined in the home agent.

10. (Currently Amended) A system, comprising:
in a terminal of a network, a first message transmission unit that is configured programmed to transmit an authenticator and [[a]] data [[unit]] to the network, the data [[unit]] including information relating to the manner in which the authenticator is formed; and
a checking unit device that is configured programmed to determine a check value with aid of the data [[unit]],

where

the terminal of the network comprises an identification unit device, which receives as input a challenge from which a response and a key are defined substantially in a same manner as in a subscriber identity module of a known mobile communications system,

the system includes a generating unit device that is configured programmed to generate authentication data blocks in the same manner as in the mobile communications system, the authentication data blocks include a challenge, a response and a key,

the system includes a transmission unit device that is configured programmed to transmit challenges contained by the authentication data blocks to the terminal,

the terminal includes a selection unit device that is configured programmed to select one challenge for use,

the first message transmission unit device inserts a value into the data {[unit]} which indicates which key corresponding to which challenge was selected for use in the terminal, and

the first message transmission unit device determines the authenticator and the checking unit device determines the check value based on the selected key.

11. (Currently Amended) The system as defined in claim 10, where the identification unit device located in connection with the terminal is a subscriber identity module used in the mobile communications system.

12. (Currently Amended) The system as defined in claim 10, where the generating unit device includes an authentication center of the mobile communications system.

13. (Currently Amended) The system as defined in claim 10, where the transmission unit device comprises a unit device for carrying out a short message switching service.

14. (Currently Amended) A method, comprising:

generating with a computer a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key;

transmitting with a transmitter at least some of the challenges contained in the authentication data

blocks to a terminal;
choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification unit device of the terminal;
receiving an authenticator and [[a]] data [[unit]] containing information relating to a manner in which the authenticator is formed from the terminal;
determining based on said data [[unit]] which challenge was chosen by the terminal;
and
determining a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator.

15. (Currently Amended) The method as defined in claim 14, where said data [[unit]] is a security parameter index in a registration message of a mobile internet protocol.

16. (Currently Amended) The method as defined in claim 14, where said data [[unit]] comprises the response corresponding to the chosen challenge.

17. (Currently Amended) A method, comprising:
receiving with a receiver a set of challenges from a telecommunications network, where each one of the challenges is contained in an authentication data block comprising said one of said challenges, a response and a key;
choosing one challenge from the set of challenges;
determining a response and a key based on the chosen challenge;
determining an authenticator based on the key corresponding to the chosen challenge;
transmitting with a transmitter said authenticator and [[a]] data [[unit]] to the telecommunications network, said data [[unit]] relating to the manner in which the authenticator is formed; and
notifying the telecommunications network of the chosen challenge, where a check value is determined with the key corresponding to the chosen challenge and said check value is compared with the authenticator.

18. (Currently Amended) The method as defined in claim 17, where said data [[unit]] is a security

parameter index in a registration message of a mobile internet protocol.

19. (Currently Amended) The method as defined in claim 17, where said data [[unit]] comprises the response corresponding to the chosen challenge.

20. (Currently Amended) An apparatus comprising:
a generator that is configured programmed to generate a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key;
a transmitter that is configured programmed to transmit at least some of the challenges contained in the authentication data blocks to a terminal;
a processor that is configured programmed to choose one of the challenges for use in the terminal, and based on the challenge, to determine a response and a key to be used with an aid of an identification unit device of the terminal;
a receiver that is configured programmed to receive an authenticator and [[a]] data [[unit]] containing information relating to a manner in which the authenticator is formed;
a first determiner that is configured programmed to determine based on said data [[unit]] which challenge was chosen by the terminal; and
a second determiner that is configured programmed to determine a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator.

21. (Currently Amended) An apparatus, comprising:
a receiver that is configured programmed to receive a set of challenges from a telecommunications network, where each one of the challenges is contained in an authentication data block comprising said one of said challenges, a response and key;
a selector that is configured programmed to choose one challenge from the set of challenges;
a first determiner that is configured to determine a response and a key based on the chosen challenge;
a second determiner that is configured programmed to determine an authenticator based on the key corresponding to the chosen challenge; and
a transmitter that is configured programmed to transmit said authenticator and [[a]] data [[unit]]

to the telecommunications network, said data [[unit]] relating to the manner in which the authenticator is formed and to notify the telecommunications network of the chosen challenge, where a check value is determined with the key corresponding to the chosen challenge and said check value is compared with the authenticator.

22. (Currently Amended) An apparatus, comprising:

generating means for generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key,

where the generation is performed in the same manner as in a known mobile communications system;

transmitting means for transmitting at least some of the challenges contained in the authentication data blocks to the terminal;

choosing means for choosing one of the challenges for use in the terminal, and

based on the challenge, determining a response and a key to be used with an aid of an identification unit device of the terminal essentially in the same way as in a subscriber identification module of the mobile communication system;

determining means for determining an authenticator with an aid of the chosen key in the terminal;

transmitting means for transmitting from the terminal to the network authenticator and [[a]] data [[unit]], the data [[unit]] containing information relating to the manner in which the authentication is formed and notifying the network with the aid of the data [[unit]] of which key corresponding to which challenge was chosen, and a check value with the aid of the chosen key in the network; and

comparing means for comparing the check value with the authenticator.

23. (Currently Amended) An apparatus, comprising:

receiving means for receiving a set of challenges from a telecommunications network, wherein where each one of the challenges is contained in an authentication data block comprising said one of said challenges, a response and a key;

choosing means for choosing one challenge from the set of challenges;

determining means for determining a response and a key based on the chosen challenge;

determining means for determining an authenticator based on the key corresponding to the chosen challenge;
transmitting means for transmitting said authenticator and [[a]] data [[unit]] to the telecommunications network, said data [[unit]] relating to the manner in which the authenticator is formed; and
notifying means for notifying the telecommunications network of the chosen challenge, where a check value is determined with the key corresponding to the chosen challenge and said check value is compared with the authenticator.

24. (Currently Amended) A computer program embodied on a computer-readable medium, where execution of the computer program controls at least one processor to perform:
generating with said at least one processor a set of subscriber-specific authentication data blocks into a network, each data block containing a challenge, a response and a key, where the generation is performed in the same manner as in a known mobile communications system;
transmitting with a transmitter at least some of the challenges contained in the authentication data blocks to a terminal;
choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification [[unit]] device of the terminal substantially in the same way as in a subscriber identification module of the mobile communication system;
determining an authentication with an aid of the chosen key in the terminal;
transmitting with a terminal transmitter, from the terminal to the network, the authenticator and [[a]] data [[unit]],
the data [[unit]] containing information relating to the manner in which the authentication is formed and notifying the network with the aid of the data [[unit]] of which key corresponding to which challenge was chosen, and a check value with the aid of the chosen key in the network; and
comparing the check value with the authenticator.

25. (Currently Amended) A computer program embodied on a computer-readable medium, where execution of the computer program controls at least one processor to perform:

generating with said at least one processor a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key;
transmitting with a transmitter at least some of the challenges contained in the authentication data blocks to a terminal;
choosing one of the challenges for use in the terminal and based on the challenge, determining a response and a key to be used with an aid of an identification [[unit]] of the terminal;
receiving with a receiver an authenticator and [[a]] data [[unit]] containing information relating to a manner in which the authenticator is formed from the terminal;
determining based on said data [[unit]] which challenge was chosen by the terminal, and
determining a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator.

26. (Currently Amended) A computer program embodied on a computer-readable medium, where execution of the computer program controls at least one processor to perform:
receiving with a receiver a set of challenges from a telecommunications network, where each one of the challenges is contained in an authentication data block comprising said one of said challenges, a response and key;
choosing with said at least one processor one challenge from the set of challenges;
determining a response and a key based on the chosen challenge;
determining an authenticator based on the key corresponding to the chosen challenge;
transmitting with a transmitter said authenticator and [[a]] data [[unit]] to the telecommunications network, said data [[unit]] relating to the manner in which the authenticator is formed; and
notifying the telecommunications network of the chosen challenge, where a check value is determined with the key corresponding to the chosen challenge and said check value is compared with the authenticator.

27. (Currently Amended) The apparatus as defined in claim 20, where the data [[unit]] is a security parameter index in a registration message of a mobile internet protocol.

28. (Currently Amended) The apparatus as defined in claim 20, where the value of the response

determined at the terminal is inserted into the data [[unit]].

29. (Currently Amended) The apparatus as defined in claim 20, where the challenges are sorted in an order at the terminal with the aid of predetermined sorting criteria, and a consecutive number corresponding to the chosen challenge is inserted into the data [[unit]].

30. (Previously Amended) The apparatus as defined in claim 20, where the challenges to be transmitted to the terminal are transmitted in an internet protocol datagram to be sent through an internet protocol network.

31. (Currently Amended) The apparatus as defined in claim 21, where the data [[unit]] is a security parameter index in a registration message of a mobile internet protocol.

32. (Currently Amended) The apparatus as defined in claim 21, where the value of the response determined at the terminal is inserted into the data [[unit]].

33. (Currently Amended) The apparatus as defined in claim 21, where the challenges are sorted in an order at the terminal with the aid of predetermined sorting criteria, and a consecutive number corresponding to the chosen challenge is inserted into the data [[unit]].

34. (Previously Amended) The apparatus as defined in claim 21, where the challenges transmitted to the terminal are transmitted by using a short message switching service.

35. (Previously Amended) The apparatus as defined in claim 21, where the challenges transmitted to the terminal are transmitted in an internet protocol datagram through an internet protocol network.